IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re application of: Murthy, et al.	§	Attorney Docket No. 26530.22
	§	
	§	Customer No. 27683
Serial No. 09/690,110	§	
	§	Group Art Unit: 2132
Filed: October 16, 2000	§	
	§	Examiner: Gurshman, Grigory
For: AN ASYMMETRIC SYSTEM AND METHOD FOR TAMPER-PROOF STORAGE OF AN AUDIT TRAIL FOR A DATABASE	§	

EXPRESS MAIL NO. EV622992627US

DATE OF DEPOSIT: July 20, 2005

This paper and fee are being deposited with the U.S. Postal Service Express Mail Post Office to Addressee service under 37 CFR §1.10 on the date indicated above and is addressed to Mail Stop Appeal Brief – Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Karen L. Underwood

Karen L. Underwood

BRIEF ON APPEAL

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

This Brief is submitted in connection with an appeal from the final rejection of the Examiner, dated January 21, 2005, finally rejecting claims 1-21, all of the pending claims in this application. Two additional copies of this Brief are also submitted.

REAL PARTY IN INTEREST

The real party in interest is NOVELL, INC., a United States company having a principal office and place of business at 1800 South Novell Place, Provo, UT 84606.

RELATED APPEALS AND INTERFERENCES

There are no related appeals and no related interferences regarding the above-identified patent application.

STATUS OF CLAIMS

Claims 1-21 are pending, stand finally rejected, and are on appeal here. Claims 1-21 are set forth in Appendix A attached hereto.

STATUS OF AMENDMENTS AFTER FINAL REJECTION

A Response to Final Office Action was filed March 21, 2005, in which arguments were presented and claims 12-16 were amended. As noted in the Advisory Action mailed April 12, 2005, the amendments was entered for purposes of appeal.

SUMMARY OF THE INVENTION

The present invention, as set forth in independent claim 1, relates to a method for providing one or more independent auditors an audit trail having one or more records for a database system. The database system includes a writing machine (writer) (Figure 1, element 16) that is not under the control of an access privileged user or auditors. Each of the audit trail records has a corresponding authentication token and a validation token (Page 3, Line27-Page 4, Line 2). The audit trail is initiated by generating an initial value of an authentication token and an initial value of a validation token based on a first encryption key of a first type (writer public key) generated by the writer and a second encryption key of the first type generated by each Auditor (auditor public key) (Page 4, Lines 6-11; Page 9, Lines 19-21; Page 9, Lines 17-27; and Page 12, Lines 4-17). A third encryption key of a second type (writer private key) is generated related to the first encryption key and a fourth encryption key of a second type (auditor private key) related to the second encryption key (Page 4, Lines 12-14; and Page 11, Lines 13-16). The

values of the writer private key, the authentication token, and the validation token for each additional audit trail record are updated and integrated into each corresponding record of the audit trail (Page 4, Lines 14-17; Page 12, Line 26-Page 13, Line 15). The auditor validates each record of the audit trail by comparing the integrated validation token with a newly computed validation token in order to detect a tampering of the audit trail (Page 4, Lines 20-23; and Page 13, Lines 18-25).

Another embodiment, as set forth in claim 7, relates to a method for providing at least one independent auditor an audit trail having one or more records recording actions taken against a database system. The integrity of the audit trail is vulnerable to actions taken by an access-privileged user other than the auditor. The database system has a writing machine (writer) not under the control of the access-privileged user or the auditor. The method includes integrating into each record a corresponding value of a validation token generated based on a first pair of public-private encryption keys generated by the writer and a second pair of public-private encryption keys generated by the auditor (Page 4, Lines 14-17; and Page 12, Line 26-Page 13, Line 15). The writer has an access to the public encryption key of the second pair (auditor public key), and the auditor has an access to the public encryption key of the first pair (writer public key). Only the writer has an access to the private key of the first pair (writer private key), and only the auditor has an access to the private key of the second pair (auditor private key) (Page 4, Lines 17-20; Page 10, Lines 15-17; and Page 11, Line 15). The auditor has the ability to compute the values of the validation token for the records to verify against the integrated values of the validation token in order to detect a tampering of the audit trail by the access-privileged user (Page 4, Lines 20-23; and Page 13, Lines 18-25).

Another embodiment, as set forth in claim 12, relates to a computer readable medium storing a computer program for providing at least one independent auditor an audit trail. The audit trail has one or more records recording actions taken against a database system. The integrity of the audit trail is vulnerable to actions taken by an access-privileged user other than the auditor. The database system has a writing machine (writer) not under the control of the access-privileged user or the auditor. The computer program has instructions for integrating into each record a corresponding value of a validation token generated based on a first pair of public-private encryption keys generated by the writer and a second pair of public-private encryption

keys generated by the auditor (Page 4, Lines 14-17; and Page 12, Line 26-Page 13, Line 15). The writer has an access to the public encryption key of the second pair (auditor public key), and the auditor has an access to the public encryption key of the first pair (writer public key). Only the writer has an access to the private key of the first pair (writer private key), and only the auditor has an access to the private key of the second pair (auditor private key) (Page 4, Lines 17-20; Page 10, Lines 15-17; and Page 11, Line 15). The auditor has the ability to compute the values of the validation token for the records to verify against the integrated values of the validation token in order to detect a tampering of the audit trail by the access-privileged user (Page 4, Lines 20-23; and Page 13, Lines 18-25).

Another embodiment, as set forth in claim 17, relates to a system for providing at least one independent auditor an audit trail. The audit trail has one or more records recording actions taken against a database. The integrity of the audit trail is vulnerable to actions taken by an access-privileged user other than the auditor. The database has a writing machine (writer) not under the control of the access-privileged user or the auditor. The system includes means for integrating into each record a corresponding value of a validation token generated based on a first pair of public-private encryption keys generated by the writer and a second pair of public-private encryption keys generated by the auditor (Page 4, Lines 14-17; and Page 12, Line 26-Page 13, Line 15). The writer has an access to the public encryption key of the second pair (auditor public key), and the auditor has an access to the public encryption key of the first pair (writer public key). Only the writer has an access to the private key of the first pair (writer private key), and only the auditor has an access to the private key of the second pair (auditor private key) (Page 4, Lines 17-20; Page 10, Lines 15-17; and Page 11, Line 15). The auditor has the ability to compute the values of the validation token for the records to verify against the integrated values of the validation token in order to detect a tampering of the audit trail by the access-privileged user (Page 4, Lines 20-23; and Page 13, Lines 18-25).

ISSUE

I. Whether claims 1-21 are unpatentable under 35 U.S.C. § 103(a) over U.S. Patent No. 6,122,630 to Strickler ("Strickler") in view of U.S. Patent No. 5,661,803 to Cordery ("Cordery").

GROUPING OF CLAIMS

As to the rejection of claims 1-6, it is Applicants' intention that solely for the purposes of this appeal, the rejected claims stand or fall together.

As to the rejection of claims 7-21, it is Applicants' intention that solely for the purposes of this appeal, the rejected claims stand or fall together.

ARGUMENT

ISSUE 1

The first issue for the Board's consideration is whether claims 1-21 are unpatentable under 35 U.S.C. §103(a) over Strickler in view of Cordery. This issue will be discussed with reference to the above identified claim groups.

As detailed below, the Applicant believes that the Examiner has improperly applied the combination of references to claims 1, 7, 12, and 17. More specifically, it is Applicant's belief that the Examiner cannot factually support a prima facie case of obviousness with respect to claims 1, 7, 12, and 17 because the references, even when combined, fail to teach or suggest the claimed subject matter.

Claims 1-6

Applicants traverse the rejection of these claims on the grounds that the references are defective in establishing a prima facie case of obviousness. It is well settled that, in order to reject a patent application for obviousness, the prior art reference must teach or suggest all of the claimed limitations. *In re Royka*, 490 F.2d 981, 180 USPQ 580 (CCPA 1974). Moreover, all words in a claim must be considered in judging the patentability of that claim against the prior art. *In re Wilson*, 424 F.2d 1382, 1385, 165 USPQ 494, 496 (CCPA 1970). Applicants respectfully submit that even if combined, Strickler and Cordery clearly do not teach or suggest the limitations of claims 1-6.

With respect to the improper application of Strickler and Cordery, the Applicant submits that neither Strickler nor Cordery, separately or in combination, teach or suggest all of the

elements of claim 1 as required by MPEP § 2143. Applicants traverse the rejection of this claim on the grounds that the references are defective in establishing a prima facie case of obviousness.

Claim 1 recites:

A method for providing one or more independent auditors an audit trail having one or more records for a database system, an integrity of the audit trail being vulnerable to actions taken by an access-privileged user other than the auditors, the database system having a writing machine (writer) not under the control of the access-privileged user or the auditors, each record having a corresponding authentication token and a validation token, the method comprising:

initiating the audit trail by generating an initial value of an authentication token and an initial value of a validation token based on a first encryption key of a first type (writer public key) generated by the writer and a second encryption key of the first type generated by each Auditor (auditor public key);

generating a third encryption key of a second type (writer private key) related to the first encryption key and a fourth encryption key of a second type (auditor private key) related to the second encryption key;

updating the values of the writer private key, the authentication token, and the validation token for each additional audit trail record and integrating the updated values of the validation token and the writer public key into each corresponding record of the audit trail; and

validating, by the auditor, each record of the audit trail by comparing the integrated validation token with a newly computed validation token in order to detect a tampering of the audit trail.

To establish a prima facie case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations.

The MPEP § 2142 provides:

> ... The examiner bears the initial burden of factually supporting any prima facie conclusion of obviousness. If the examiner does not produce a prima facie case, the applicant is under no obligation to submit evidence of nonobviousness...

It is submitted that, in the present case, the Examiner has not factually supported a prima facie case of obviousness.

Strickler and Cordery cannot be applied to reject claim 1 under 35 U.S.C. § 103 which provides that:

> A patent may not be obtained ... if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which the subject matter pertains ... (Emphasis added)

Thus, when evaluating a claim for determining obviousness, all limitations of the claim must be evaluated. The examiner indicates that Figure 6 of Strickler discloses the method step of "initiating the audit trail by generating an initial value of an authentication token and an initial value of a validation token." Applicants respectfully disagree. Contrary to the Examiner's assertion, Strickler does not teach or suggest a method of "initiating the audit trail by generating an initial value of an authentication token" *and* an "initial value of a validation token" based on a "first encryption key of a first type (writer public key) generated by the writer and a second encryption key of the first type generated by each Auditor (auditor public key)". Strickler generally describes an a priori audit token but neither describes or suggests generating an initial authentication token and an initial validation token for the audit trail. The Examiner does not indicate whether the a priori token of Strickler allegedly discloses the validation token or the authentication token of the subject claim. However, the a priori token of Strickler is clearly insufficient to disclose generation of both "an initial value of an authentication token and an initial value of a validation token." The Examiner makes no allegation, and Applicants are unaware, of any description or suggestion provided by Cordery for generation of "an initial value of an authentication token and an initial value of a validation token." Thus, Strickler and Cordery, alone or in combination, do not teach each and every element of claim 1. For at least this reason, Strickler and Cordery are insufficient to obviate claim 1.

The Examiner apparently alleges that Cordery provides for the deficiencies of Strickler by disclosing independent keys used for generating digital tokens. Applicants respectfully disagree. Cordery generally describes digital meters that generate independent keys. Cordery in no manner describes or suggests a mechanism for generating an initial value of an authentication token and a validation token from "a first encryption key of a first type...generated by a writer" and "a second encryption key of the first type generated by each Auditor" and is wholly silent with regard to any encryption key generation performed by an auditor. Thus, Cordery is clearly insufficient to provide for the deficiencies of Strickler. Thus, Strickler and Cordery fail to describe or suggest a mechanism for generating an authentication token and a validation token from "a first encryption key of a first type" that is "generated by the writer" and a second encryption key of the first type generated by each Auditor." For at least this reason, Strickler and Cordery are insufficient to obviate claim 1.

With regard to the claim 1 limitation of "generating a third encryption key of a second type (writer private key) related to the first encryption key and a fourth encryption key of a second type (auditor private key) related to the second encryption key," the Examiner has not even alleged that Strickler or Cordery teach or suggest such a method step. Applicants submit that no such teaching or suggestion is provided by either Strickler or Cordery, and for at least this reason, Strickler and Cordery are insufficient to provide a prima facie case of obviousness with regard to the claim 1 limitations. Thus, Strickler and Cordery are insufficient to obviate claim 1.

With regard to the claim 1 limitation of "updating the values of the writer private key, the authentication token, and the validation token for each additional audit trail record and integrating the updated values of the validation token and the writer public key into each corresponding record of the audit trail," the Examiner has not even alleged that either Strickler or Cordery describe or suggest the limitation of "updating the values of the writer private key, the authentication token, and the validation token of each additional audit trail record." Applicants submit that no such teaching or suggestion is provided by either Strickler or Cordery, and for at least this reason, Strickler and Cordery are insufficient to provide a prima facie case of obviousness with regard to the claim 1 limitations. Thus, Strickler and Cordery are insufficient to obviate claim 1.

With further regard to the claim 1 limitation of "updating the values of the writer private key, the authentication token, and the validation token for each additional audit trail record and integrating the updated values of the validation token and the writer public key into each corresponding record of the audit trail," the Examiner alleges that Strickler describes a method of integrating the updated values of the validation token and the writer public key into each corresponding record of the audit trail in Figures 10a and 10b. Apparently the Examiner alleges that inclusion of a "TRANID" included in an audit trail discloses the subject method step of "integrating the updated values of the validation token and the writer public key into each corresponding record of the audit trail." Applicants respectfully disagree. As recited in the subject claim 1 limitation of "initiating the audit trail," the initial values of the authentication and validation tokens are generated "based on a first encryption key...generated by the writer" and a "second encryption key...generated by each Auditor." The TRANID, as described by Strickler, simply comprises a transaction identifier that is unique (See, for example, Strickler, Column 12, Lines 16-23). No description or suggestion is provided by Strickler for generating TRANIDs "based on a first encryption key...generated by the writer" and a "second encryption key...generated by each Auditor" Thus, storage of a TRANID in a record as shown by Strickler is clearly insufficient to obviate the subject claim limitation of "integrating the updated values of the validation token and the writer public key into each corresponding record of the audit trail" because the authentication and validation tokens are expressly recited in claim 1 as being generated based on "a first encryption key...generated by the writer" and a "second encryption key...generated by each Auditor" – a mechanism not described, suggested, or otherwise alluded to as being involved in the creation of a TRANID by Strickler. For at least this reason, Strickler and Cordery are insufficient to provide a prima facie case of obviousness with regard to the claim 1 limitations. Thus, Strickler and Cordery are insufficient to obviate claim 1.

With regard to the claim 1 limitation of "validating, by the auditor, each record of the audit trail by comparing the integrated validation token with a newly computed validation token in order to detect a tampering of the audit trail," the Examiner alleges that the TRANIDs are representative of the integrated tokens. Applicants respectfully disagree. As noted above, Strickler only describes the TRANIDs as transaction identifiers that are unique. No description or suggestion is provided by Strickler for generating TRANIDs "based on a first encryption

key...generated by the writer" and a "second encryption key...generated by each Auditor." Thus, comparison of TRANIDs, as described by Strickler, is wholly insufficient to disclose validating each record of the audit trail by "comparing the integrated validation token with a newly computed validation token." For at least this reason, Strickler and Cordery are insufficient to provide a prima facie case of obviousness with regard to the claim 1 limitations. Thus, Strickler and Cordery are insufficient to obviate claim 1.

Claims 2-6 depend from and further limit claim 1. For the reasons described above, Strickler and Cordery do not include all elements of independent claim 1 and hence fail to obviate the present invention as recited in claims 1-6.

CLAIMS 7-21

Claim 7 recites:

> A method for providing at least one independent auditor an audit trail, the audit trail having one or more records recording actions taken against a database system, the integrity of the audit trail being vulnerable to actions taken by an access-privileged user other than the auditor, the database system having a writing machine (writer) not under the control of the access-privileged user or the auditor, the method comprising:
>
> integrating into each record a corresponding value of a validation token generated based on a first pair of public-private encryption keys generated by the writer and a second pair of public-private encryption keys generated by the auditor,
>
> wherein the writer has an access to the public encryption key of the second pair (auditor public key), and the auditor has an access to the public encryption key of the first pair (writer public key),
>
> wherein only the writer has an access to the private key of the first pair (writer private key), and only the auditor has an access to the private key of the second pair (auditor private key), and
>
> wherein the auditor has the ability to compute the values of the validation token for the records to verify against the integrated values of the validation token in order to detect a tampering of the audit trail by the access-privileged user.

With regard to the claim 7 limitation of "integrating into each record a corresponding value of a validation token generated based on a first pair of public-private encryption keys generated by the writer and a second pair of public-private encryption keys generated by the auditor," the Examiner alleges Strickler discloses such a method step in Figures 10a and 10b and states that "the integrated token values are represented by TRANIDs." (Office Action dated 1/21/2005, page 5). Applicants respectfully disagree. The TRANID of Strickler is only

described as a transaction identifier that is unique (See, for example, Strickler, Column 12, Lines 16-23). No description or suggestion is provided by Strickler for generating TRANIDs "based on a first pair of public-private encryption keys generated by the writer and a second pair of public-private encryption keys generated by the auditor" Thus, the TRANIDs described by Strickler are clearly insufficient to disclose a validation token generated based on a first pair of public-private encryption keys generated by the writer and a second pair of public-private encryption keys generated by the auditor. For at least this reason, Strickler and Cordery are insufficient to provide a prima facie case of obviousness with regard to the claim 7 limitations. Thus, Strickler and Cordery are insufficient to obviate claim 7.

Additionally, the Examiner alleges that the subject claim limitation of "the auditor" is disclosed by the "consumer" (38) described by Strickler, and that the subject claim limitation of "the writer" is disclosed by the input unit (54) described by Strickler. Applicants respectfully disagree. Strickler in no manner describes or suggests that the consumer has access "to the public encryption key of the first pair (writer public key)," has "access to the private key of the second pair (auditor private key)" or has "the ability to compute the values of the validation token for the records to verify against the integrated values of the validation token" as clearly recited in regard to the auditor of the subject claim limitations. Additionally, Strickler in no manner describes or suggests that the input unit has "access to the public encryption key of the second pair (auditor public key)," or has access to the "private key of the first pair (writer private key)," as clearly recited in regard to the writer of the subject claim limitations. For at least this reason, Strickler and Cordery are insufficient to provide a prima facie case of obviousness with regard to the claim 7 limitations. Thus, Strickler and Cordery are insufficient to obviate claim 7.

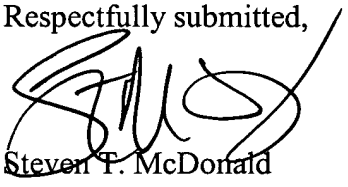
Claims 12 and 17 recite similar features as claim 7 and were rejected for the same rationale. Therefore, the same distinctions between Strickler and Cordery and the claimed invention in claim 7 apply for these claims. Claims 8-11, claims 13-16, and claims 18-21 respectively depend from and further limit claims 7, 12, and 17. For the reasons described above, Strickler and Cordery do not include all elements of independent claims 7, 12, and 17 and hence fail to obviate the present invention as recited in claims 7-21.

II. Conclusion

Accordingly, it is respectfully submitted that the references alone or in combination do not disclose or suggest the subject matter of claims 1-21.

For all of the foregoing reasons, it is respectfully submitted that claims 1-21 be allowed. A prompt notice to that effect is respectfully requested.

Respectfully submitted,



Steven T. McDonald
Registration No. 45,999

Dated: 20 July 2005

HAYNES AND BOONE, LLP
901 Main Street, Suite 3100
Dallas, Texas 75202-3789
Telephone: 972/739-8644
Facsimile: 972/692-9075
R1113000

APPENDIX A

1. A method for providing one or more independent auditors an audit trail having one or more records for a database system, an integrity of the audit trail being vulnerable to actions taken by an access-privileged user other than the auditors, the database system having a writing machine (writer) not under the control of the access-privileged user or the auditors, each record having a corresponding authentication token and a validation token, the method comprising:

initiating the audit trail by generating an initial value of an authentication token and an initial value of a validation token based on a first encryption key of a first type (writer public key) generated by the writer and a second encryption key of the first type generated by each Auditor (auditor public key);

generating a third encryption key of a second type (writer private key) related to the first encryption key and a fourth encryption key of a second type (auditor private key) related to the second encryption key;

updating the values of the writer private key, the authentication token, and the validation token for each additional audit trail record and integrating the updated values of the validation token and the writer public key into each corresponding record of the audit trail; and

validating, by the auditor, each record of the audit trail by comparing the integrated validation token with a newly computed validation token in order to detect a tampering of the audit trail.

2. The method of claim 1 wherein the step of initiating further includes storing the initial values of the validation token and the writer public key in an initial record of the audit trail.

3. The method of claim 1 wherein the step of initiating further includes:

concatenating a predetermined identity for the audit trail, and a common initialization encryption key generated by the auditor with the auditor public key and the writer public key;

generating the initial value of the validation token through at least one hashing process and at least one encryption process using the concatenated result,

wherein the initial value of the authentication token is used as an encryption key for the encryption process.

4. The method of claim 1 wherein the step of generating further includes:

storing the auditor private key in a first secured storage accessible only by the auditor; and

storing the writer private key in a second secured storage accessible only by the writer.

5. The method of claim 1 wherein the step of updating further includes:

updating the value of the writer private key;

updating the value of the writer public key based on the updated writer private key;

updating the value of the authentication token by a hashing process based on the updated value of the writer private key and the auditor public key; and

updating the value of the validation token through at least a hashing process and an encryption process,

wherein the updated authentication token is used as an encryption key for the encryption process while updating the value of the validation token.

6. The method of claim 1 wherein the newly computed validation token is generated by the auditor based on the auditor private key and the writer public key.

7. A method for providing at least one independent auditor an audit trail, the audit trail having one or more records recording actions taken against a database system, the integrity of the audit trail being vulnerable to actions taken by an access-privileged user other than the auditor, the database system having a writing machine (writer) not under the control of the access-privileged user or the auditor, the method comprising:

integrating into each record a corresponding value of a validation token generated based on a first pair of public-private encryption keys generated by the writer and a second pair of public-private encryption keys generated by the auditor,

wherein the writer has an access to the public encryption key of the second pair (auditor public key), and the auditor has an access to the public encryption key of the first pair (writer public key),

wherein only the writer has an access to the private key of the first pair (writer private key), and only the auditor has an access to the private key of the second pair (auditor private key), and

wherein the auditor has the ability to compute the values of the validation token for the records to verify against the integrated values of the validation token in order to detect a tampering of the audit trail by the access-privileged user.

8. The method of claim 7 wherein the step of integrating further includes:

initiating the audit trail by generating an initial value of the authentication token and an initial value of the validation token for an initial record of the audit trail based on the writer public key and the auditor public key; and

updating the values of the writer private key, the authentication token, and the validation token,

wherein each updated value of the validation token is integrated into a corresponding record of the audit trail.

9. The method of claim 8 wherein the step of initiating further includes:

concatenating a predetermined identity for the audit trail, and a common initialization encryption key generated by the auditor with the auditor public key and the writer public key; and

generating the initial value of the validation token through at least one hashing process and at least one encryption process using the concatenated result,

wherein the initial value of the authentication token is used as an encryption key for the encryption process.

10. The method of claim 9 wherein the step of initiating further includes:

storing the auditor private key, the identity for the audit trail, and the initial record in a designated secured information storage accessible only by the auditor,

wherein the stored auditor private key, the identity for the audit trail, and the initial record can be retrieved by the auditor and used with the writer public key accessible by the

auditor to compute the values of the validation token for the records to verify against the integrated values of the validation token.

11. The method of claim 8 wherein the step of updating further includes:

updating the value of the writer private key through a hashing process;

updating the value of the writer public key based on the updated writer private key;

updating the value of the authentication token by a hashing process based on the updated value of the writer private key; and

updating the value of the validation token through at least a hashing process and an encryption process,

wherein the updated authentication token is used as an encryption key for the encryption process while updating the value of the validation token.

12. A computer readable medium storing a computer program for providing at least one independent auditor an audit trail, the audit trail having one or more records recording actions taken against a database system, the integrity of the audit trail being vulnerable to actions taken by an access-privileged user other than the auditor, the database system having a writing machine (writer) not under the control of the access-privileged user or the auditor, the computer program comprising instructions for:

integrating into each record a corresponding value of a validation token generated based on a first pair of public-private encryption keys generated by the writer and a second pair of public-private encryption keys generated by the auditor,

wherein the writer has an access to the public encryption key of the second pair (auditor public key), and the auditor has an access to the public encryption key of the first pair (writer public key),

wherein only the writer has an access to the private key of the first pair (writer private key), and only the auditor has an access to the private key of the second pair (auditor private key), and

wherein the auditor has the ability to compute the values of the validation token for the records to verify against the integrated values of the validation token in order to detect a tampering of the audit trail by the access-privileged user.

13. The computer readable medium storing the computer program of claim 12 wherein the means for integrating further includes instructions for:

initiating the audit trail by generating an initial value of the authentication token and an initial value of the validation token for an initial record of the audit trail based on the writer public key and the auditor public key; and

updating the values of the writer private key, the authentication token, and the validation token,

wherein each updated value of the validation token is integrated into a corresponding record of the audit trail.

14. The computer readable medium storing the computer program of claim 13 wherein the means for initiating further includes instructions for:

concatenating a predetermined identity for the audit trail, and a common initialization encryption key generated by the auditor with the auditor public key and the writer public key; and

generating the initial value of the validation token through at least one hashing process and at least one encryption process using the concatenated result,

wherein the initial value of the authentication token is used as an encryption key for the encryption process.

15. The computer readable medium storing the computer program of claim 14 wherein the means for initiating further includes instructions for:

storing the auditor private key, the identity for the audit trail, and the initial record in a designated secured information storage accessible only by the auditor,

wherein the auditor private key, the identity for the audit trail, and the initial record can be retrieved by the auditor and used with the writer public key accessible by the auditor to

compute the values of the validation token for the records to verify against the integrated values of the validation token.

16. The computer readable medium storing the computer program of claim 13 wherein the means for updating further includes instructions for:

updating the value of the writer private key through a hashing process;

updating the value of the writer public key based on the updated writer private key;

updating the value of the authentication token by a hashing process based on the updated value of the writer private key; and

updating the value of the validation token through at least a hashing process and an encryption process,

wherein the updated authentication token is used as an encryption key for the encryption process while updating the value of the validation token.

17. A system for providing at least one independent auditor an audit trail, the audit trail having one or more records recording actions taken against a database, the integrity of the audit trail being vulnerable to actions taken by an access-privileged user other than the auditor, the database having a writing machine (writer) not under the control of the access-privileged user or the auditor, the system comprising means for:

integrating into each record a corresponding value of a validation token generated based on a first pair of public-private encryption keys generated by the writer and a second pair of public-private encryption keys generated by the auditor,

wherein the writer has an access to the public encryption key of the second pair (auditor public key), and the auditor has an access to the public encryption key of the first pair (writer public key),

wherein only the writer has an access to the private key of the first pair (writer private key), and only the auditor has an access to the private key of the second pair (auditor private key), and

wherein the auditor has the ability to compute the values of the validation token for the records to verify against the integrated values of the validation token in order to detect a tampering of the audit trail by the access-privileged user.

18. The system of claim 17 wherein the means for integrating further includes means for:

initiating the audit trail by generating an initial value of the authentication token and an initial value of the validation token for an initial record of the audit trail based on the writer public key and the auditor public key; and

updating the values of the writer private key, the authentication token, and the validation token,

wherein each updated value of the validation token is integrated into a corresponding record of the audit trail.

19. The system of claim 18 wherein the means for initiating further includes means for:

concatenating a predetermined identity for the audit trail, and a common initialization encryption key generated by the auditor with the auditor public key and the writer public key; and

generating the initial value of the validation token through at least one hashing process and at least one encryption process using the concatenated result,

wherein the initial value of the authentication token is used as an encryption key for the encryption process.

20. The system of claim 19 wherein the means for initiating further includes means for:

storing the auditor private key, the identity for the audit trail, and the initial record in a designated secured information storage accessible only by the auditor,

wherein the stored auditor private key, the identity for the audit trail, and the initial record can be retrieved by the auditor and used with the writer public key accessible by the auditor to compute the values of the validation token for the records to verify against the integrated values of the validation token.

21. The system of claim 18 wherein the means for updating further includes means for:

updating the value of the writer private key through a hashing process;

updating the value of the writer public key based on the updated writer private key;

updating the value of the authentication token by a hashing process based on the updated value of the writer private key; and

updating the value of the validation token through at least a hashing process and an encryption process,

wherein the updated authentication token is used as an encryption key for the encryption process while updating the value of the validation token.